# An analysis of IP Prefix Hijacking and Interception

By
Khin Thida Latt
kt-latt@jaist.ac.jp

# Target Area

- Every organization has its Internet connectivity by one protocol: BGP4 ( Border Gateway Protocol)
- This BGP4 has longstanding vulnerabilities
- Among these vulnerabilities, today presentation is about
  - "IP prefix Hijacking"
  - "Traffic Interception"

# Background Info

Prefix hijacking and traffic interception are serious threats. Why?

- AT & T WorldNet suffers outage (Dec 1999)

  leaving 1.8 million customers without Web access for almost a day

- Two weeks shutdown of all banking, government and political sites in Estonia ( May 2007)

- Kenyan Route Hijack
  - An ISP from USA and Europe, AboveNet hijacked prefix owned by Africa Online (March 2008)

# Purpose

- Analyze !
  - Many ideas have been presented to detect/prevent
  - However, no enough analysis towards both areas

  - intends this analysis would be for a stepping-stone towards solving these two threats

# Content

- Introduction
- Taxonomy of IP prefix hijacking
- Taxonomy of traffic interception
- Attack model of Traffic Interception

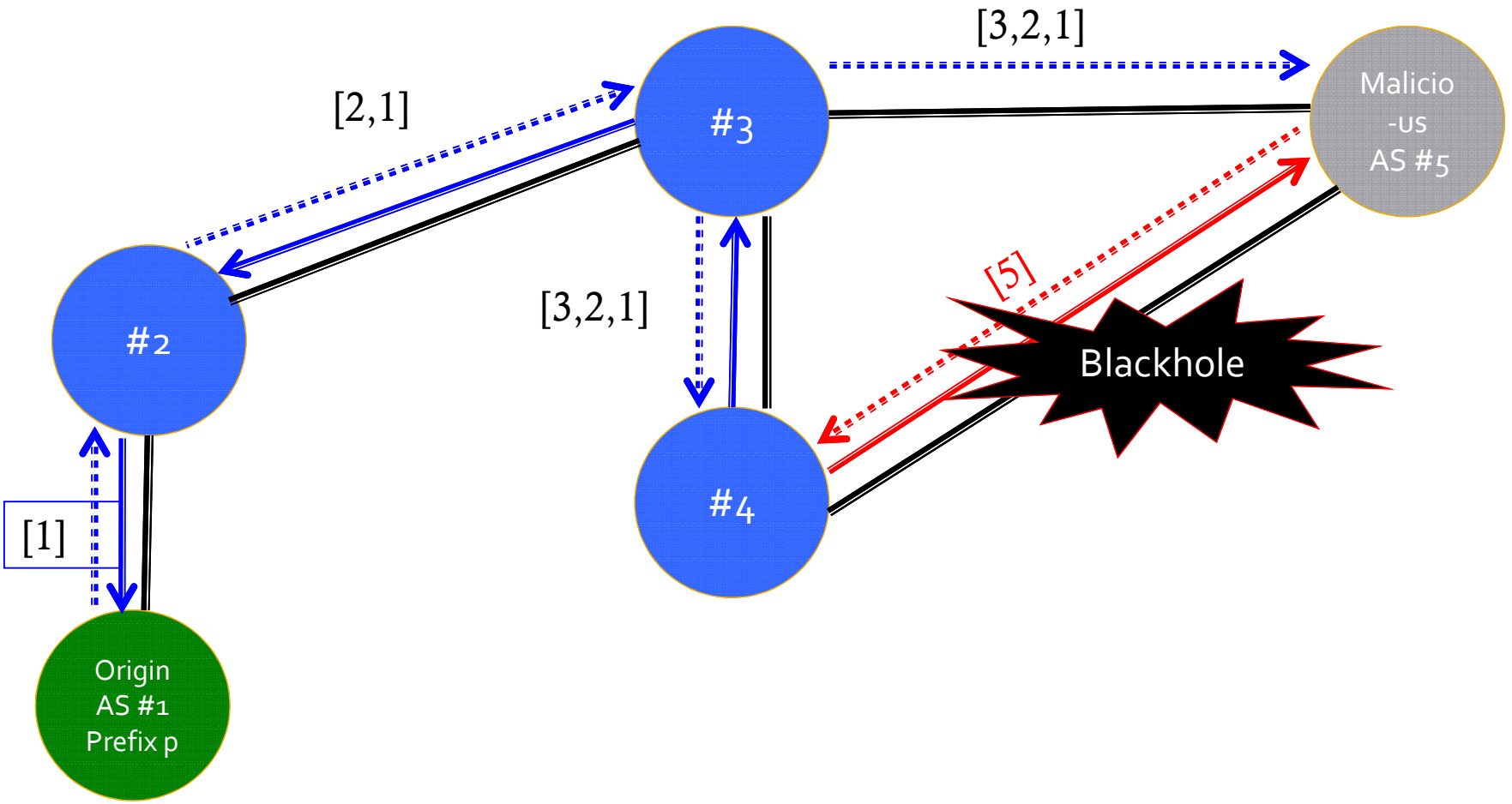
# Introduction

# Hijacking and Interception?

- What is prefix hijacking?
  - AS makes an advertisement of a prefix although it is neither prefix owner nor transit AS

- What is Traffic Interception?
  - Traffic Interception = hijacking + *forwarding*

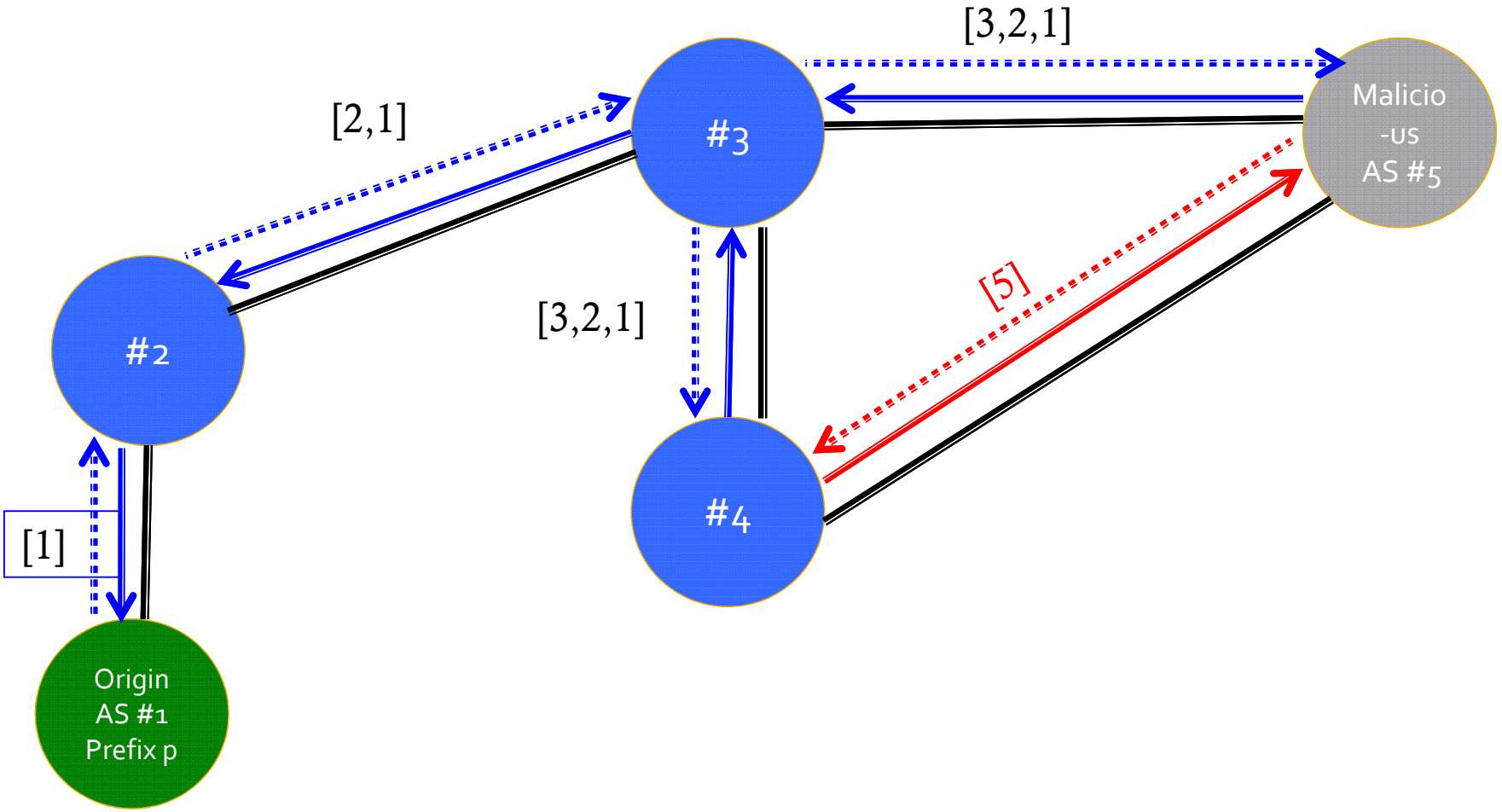
# Prefix Hijacking



# Reasons behind a hijack

- Legitimate reasons
  - Engineering traffic
- Mis-configuration
- Malicious attempts
  - Brand spoofing/phishing

# Traffic Interception



# Differences between Hijacking and Interception

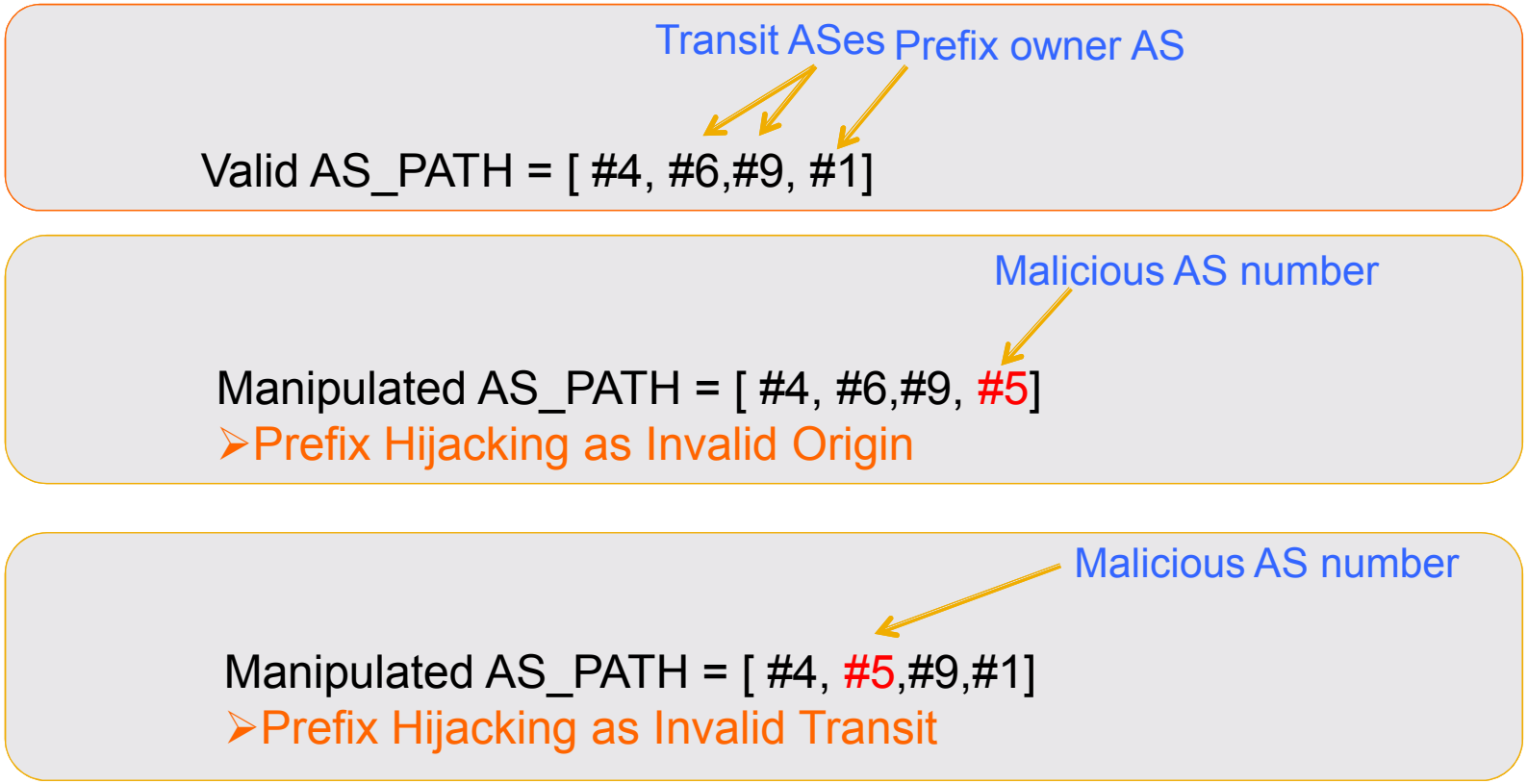
- IP prefix Hijacking
  - black-hole all the hijacked traffic
  - connectivity disrupted (Denial of Service Attack)
  - be known after black holing the traffic

- Traffic Interception
  - No black-hole
  - connectivity is not disrupted (Man-In-The-Middle Attack)
  - Transparent to the victim

# Taxonomy of Prefix Hijacking

# How does malicious AS hijack a prefix?

- By manipulating *AS_PATH attribute* of BGP update message



# Classification of Prefix Hijacking

- If Announced prefix = 150.65.0.0/16, size of the hijacked prefix can be
  1. exactly same size - *regular prefix hijacking*

150.65.0.0/16 (JAIST)

  2. more specific - *sub prefix hijacking*

150.65.117.0/24 (Shinoda-lab)

  3. Less specific - *super prefix hijacking*

150.0.0.0/8

# Some of real incidents

| Date | Incident | Classification |
|---|---|---|
| Jan. 2006 | Con-Ed Steals the Net<br><br>Con Edison (AS27506) originated several prefixes that others own. | Invalid Origin<br>Regular Prefix |
| Feb. 2008 | Youtube IP hijacking!<br><br>YouTube (AS36561) 's announced prefix = 208.65.152.0/22<br>Hijaced prefix by AS17557 = 208.65.153.0/24 | Invalid Origin<br>Sub prefix |
| Nov.2008 | Potential Prefix Hijack by Brazil AS<br><br>(AS16735) announced almost the whole Internet to two of its peers | Invalid Transit<br>Regular Prefix |

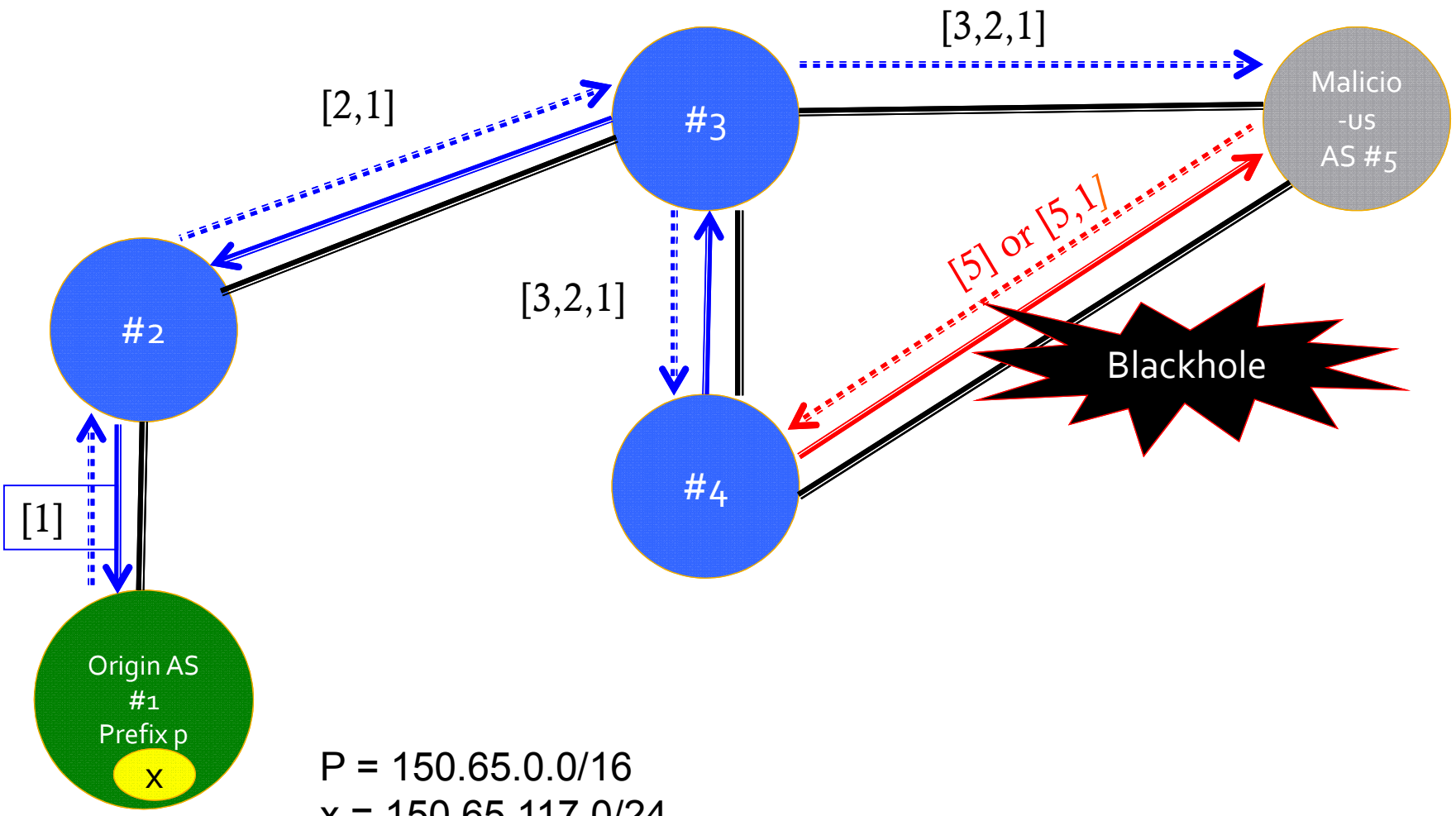
# only currently-using prefixes are hijacked?

- No!
- unused but possibly be assigned IP prefixes can also be hijacked
- Any legitimate traffic is not disrupted

# Hijacking Incidents on Unused Address Space of US DoD During 2008

| Prefix | Country | Duration | Classification |
|---|---|---|---|
| 11.11.11.0/24 | Hong Kong | 1.1 hours | Invalid Origin – Sub prefix |
| 7.7.7.0/24 | South Korea | 16.0 mins | Invalid Origin – Sub prefix |
| 11.1.1.0/24 | Russia | 3.5weeks | Invalid Origin – Sub prefix |
| 11.0.0.0/24 | US | 16.0 hours | Invalid Origin – Sub prefix |
| 30.30.30.0/24 | Argentina | 40.0 mins | Invalid Origin – Sub prefix |
| 11.1.1.0/24 | Indonesia | 2.1 mins | Invalid Origin – Sub prefix |
| 11.11.11.0/24 | Turkey | 6.5 mins | Invalid Origin – Sub prefix |

# Attack Model




P = 150.65.0.0/16
x = 150.65.117.0/24

# Recent Methods and issues

| Category | Name | Issues |
|---|---|---|
| Modify BGP | SBGP, SoBGP | Not easily deployable |
| Checking central registry | Internet Registry Data | Not up-to-date |
| Filters | PG-BGP, Bogon | Manual, high false positives/negatives rate |
| Alarm services | BGPMon, PHAS, MyASN .. etc | Sometimes not distinguishable from legitimate ones<br><br>Can detect only "Invalid Origin" Type |

# Taxonomy of Traffic Interception

# How does malicious AS intercept ?

1. Firstly, hijack the prefix
2. Then forward the hijacked traffic

- To forward the traffic, malicious AS
  - know valid route to destination
  - make ASes along valid route keep valid route ← *Key to successful interception*
  - not introduce "unreachability" to victim

# How does malicious AS maintain valid route?

- maintains valid route by itself

  OR

- prepends valid route into invalid route

➢ *Then how?*

# Attack Model

# Attack Model with shorter AS_PATH

- *Malicious AS maintains valid route by itself*

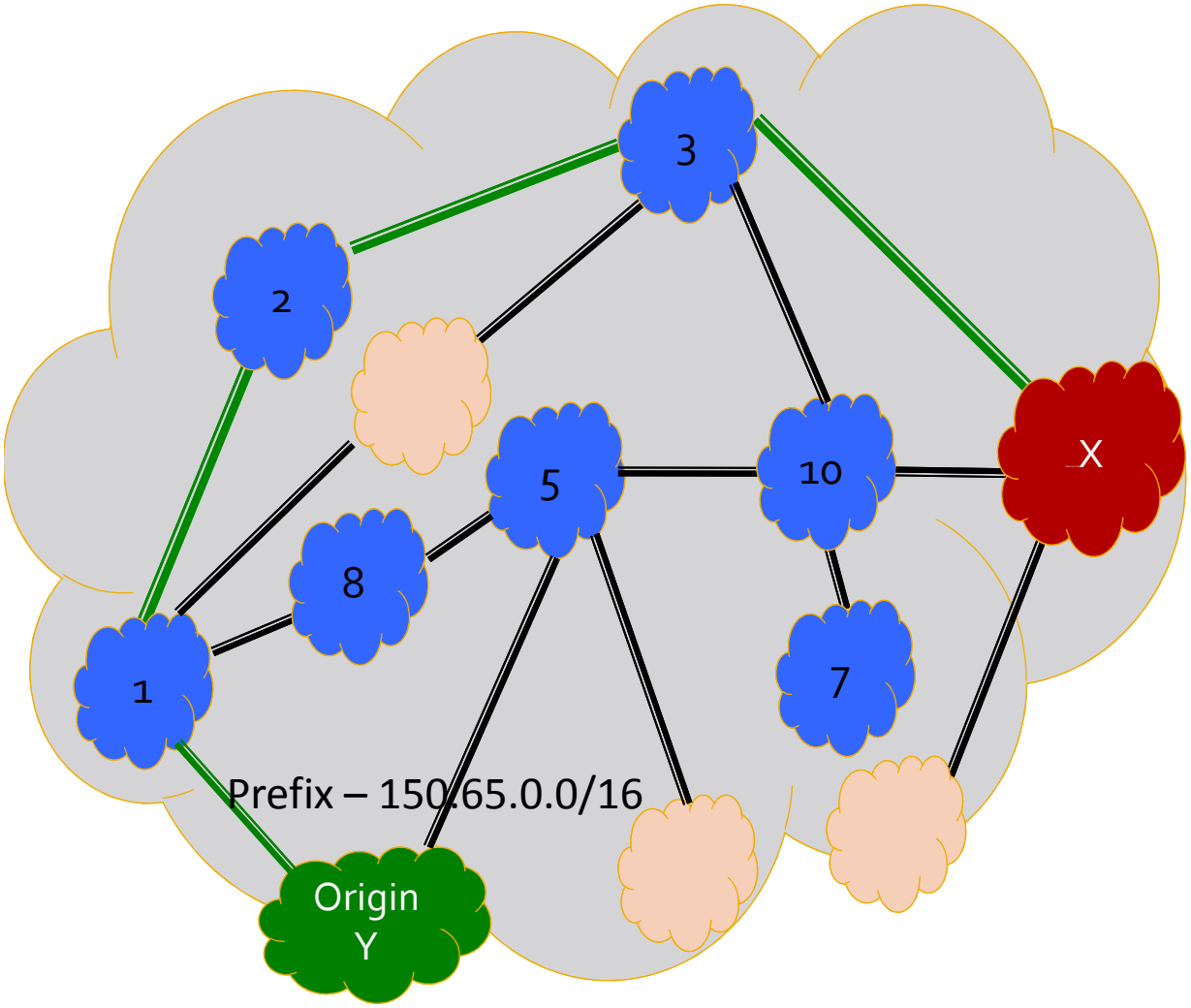
To make successful Interception, Malicious AS follows

- Valley-free nature
- AS relationships ( customer> peer> provider )

Not to introduce reachability problem

1. must carefully choose Ases to propagate invalid route
   - if existing route is through provider,
     then propagate route to peers + customers
   - else
     propagate route to all
2. must keep the valid route by itself to fwd traffic back

# Attack Model with shorter AS_PATH




**AS #X**
announced prefix = 150.65.10.0/24 (or) /16
maintained Path = [3,2,1,Y]
Announced path = [X,1,Y]

**AS #10**
install best path = [X,1,Y]

**AS #7**
install best path = [10,X,1,Y]

# Hint to detect!

- Hint : hiding hops between itself and Origin AS shows "strange edge"
- "edge" means "relationship"
- "Strange edge" means "strange relationship"
- Strange relationship is the relationship that
  - Violates valley free nature
  - Introduces a big gap between two Ases

  - Then how to explore relationships among ASes?

# How to explore relationships?

- Infer the relationships using route-view data
- Inferring based on degree of ASes + traffic size of Ases (currently doing)

# Attack Model with longer AS_PATH

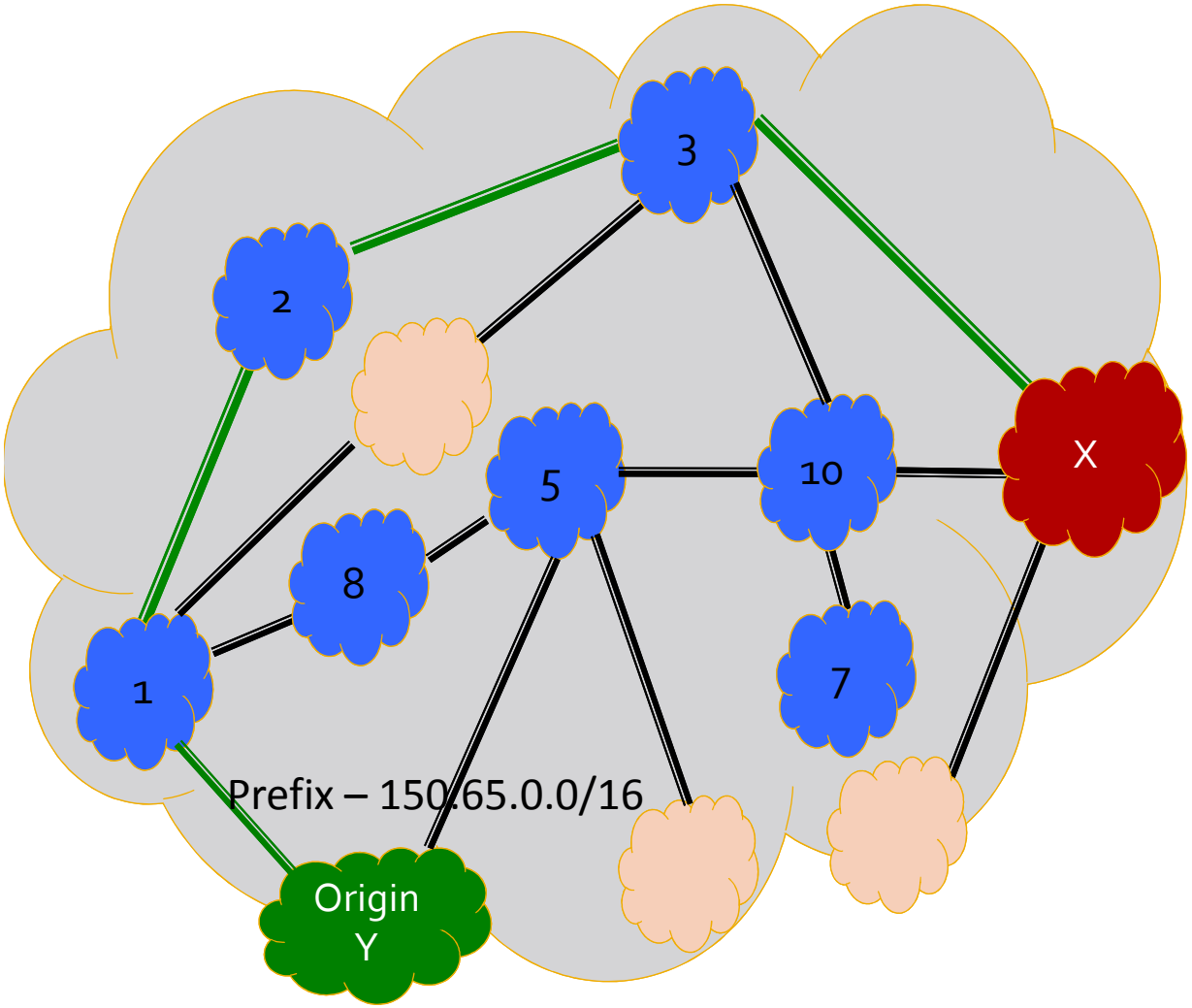
- *Malicious AS does not maintain valid route by itself*

To make successful Interception, malicious AS

1. Need not consider to which ASes invalid route should propagated

2. Need not keep the valid route by itself
   - Just prepend valid route to invalid route
     - Taking advantage of "loop prevention mechanism"

# Attack Model with longer AS_PATH




**AS #X**
announced prefix = 150.65.10.0/24
announced Path = [X,3,2,1,Y]

**AS #3**
- discard [X,3,2,1,Y] *(AS loop)*

**AS #10**
- install best path = [X,3,2,1,Y]

**AS #7**
- install best path = [10,X,3,2,1,Y]

# Hints to detect!

- Hint-1 : can intercept only “sub” prefix
- Hint-2 : taking advantage of “loop prevention mechanism”
- These hints can be found in discarded paths
- To do -> check NLRI + AS_PATH in discarded paths

# Summary

- Still no sol: towards interception
- Analysis/attack model give hints towards solution
- What kind of hints?
  - Attack model with shorter AS_PATH
    - malicious AS hides one or more Ases -> leads to strange edge
  - Attack model with longer AS_PATH
    - it takes ad of loop prevention mechanism -> should we check before discarding route?

# Any Question?